СТРАТЕГИЧЕСКАЯ ТЯЖБА



№22, 2016

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ БЮЛЛЕТЕНЬ
ГОМЕЛЬСКОГО ЦЕНТРА СТРАТЕГИЧЕСКОЙ ТЯЖБЫ

В данном номере бюллетеня «Стратегическая тяжба» опубликованы выдержки доклада международной неправительственной организации Amnesty International «Достаточно осознавать, что она есть»: гражданское общество, секретность и слежка в Беларуси». С полным текстом доклада можно ознакомиться на сайте данной организации https://www.amnesty.org/en/documents/eur49/4306/2016/ru/

О ГЛАВНОМ



ДОСТАТОЧНО ОСОЗНАВАТЬ, ЧТО ОНА ЕСТЬ: ГРАЖДАНСКОЕ ОБЩЕСТВО, СЕКРЕТНОСТЬ И СЛЕЖКА В БЕЛАРУСИ

4. СКОВЫВАЮЩИЙ ЭФФЕКТ: ЖИЗНЬ В УСЛОВИЯХ СЛЕЖКИ

Опасения по поводу слежки широко распространены среди активистов гражданского общества в Беларуси, и даже среди тех, кто живёт в изгнании. Недостаточные меры по регулированию и надзору, отсутствие возможности оспорить слежку означают, что у активистов просто нет другого выбора, кроме как предположить, что за ними постоянно следят. Поскольку за многие законные виды деятельности – в том числе журналистскую работу без правительственной аккредитации, работу в незарегистрированной организации или за участие в мирной несанкционированной демонстрации – в Беларуси предусмотрена административная или даже уголовная ответственность, активисты зачастую опасаются, что слежка за их повседневной деятельностью может подвергнуть их опасности судебного преследования[…].

4.1 ПОВСЕМЕСТНЫЕ ПОДОЗРЕНИЯ В ИСПОЛЬЗОВАНИИ СЛЕЖКИ

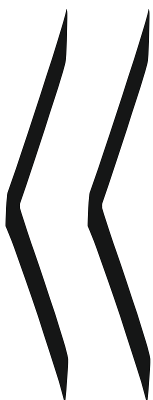
[…]В деле Роман Захаров против России, Европейский суд по правам человека отметил, что тайная слежка может нанести ущерб правам даже тех людей, которые не являлись её объектами. ЕСПЧ указал, что там, где система тайной слежки может отразиться на любом человеке и там, где не имеется соответствующих средств правовой защиты для того, чтобы оспорить предполагаемое тайное наблюдение: «НЕЛЬЗЯ ГОВОРИТЬ О ТОМ, ЧТО ШИРОКОМАСШТАБНЫЕ ПОДОЗРЕНИЯ И ОЗАБОЧЕННОСТЬ В ОБЩЕСТВЕ ПО ПОВОДУ ЗЛОУПОТРЕБЛЕНИЙ ПОЛНОМОЧИЯМИ ПО ОСУЩЕСТВЛЕНИЮ СЕКРЕТНОЙ СЛЕЖКИ ЯВЛЯЮТСЯ НЕОПРАВДАННЫМИ[…]. В ПОДОБНЫХ ОБСТОЯТЕЛЬСТВАХ ДАННАЯ УГРОЗА САМА ПО СЕБЕ МОЖЕТ ОГРАНИЧИТЬ СВОБОДНЫЙ ОБМЕН ИНФОРМАЦИЕЙ ЧЕРЕЗ ПОЧТОВЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СЕРВИСЫ, ТЕМ САМЫМ ПРЕДСТАВЛЯЯ ДЛЯ ВСЕХ ПОЛЬЗОВАТЕЛЕЙ ИЛИ ПОТЕНЦИАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ ПРЯМОЕ ВМЕШАТЕЛЬСТВО В ИХ ПРАВО [НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ И СЕМЕЙНОЙ ЖИЗНИ]»[…].

2 стр. >>>



ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ БЮЛЛЕТЕНЬ ГОМЕЛЬСКОГО ЦЕНТРА СТРАТЕГИЧЕСКОЙ ТЯЖБЫ

ДОСТАТОЧНО ОСОЗНАВАТЬ, ЧТО ОНА ЕСТЬ: ГРАЖДАНСКОЕ ОБЩЕСТВО, СЕКРЕТНОСТЬ И СЛЕЖКА В БЕЛАРУСИ



4.2 КАК ОБЩАТЬСЯ

Если жить в постоянном страхе перед слежкой, то многие простые повседневные действия создают серьёзные трудности, особенно для активистов. Например, большинство людей, говоривших с Amnesty International, подчёркивали, что не доверяют большинству средств коммуникации, и предпочитают встречаться лицом к лицу, чтобы обсуждать свою работу, в том числе особо важные вопросы[…].

4.3 КАК ВСТРЕЧАТЬСЯ

Наряду с тем, что страх перед опасностью слежки, распространённый среди активистов гражданского общества, делает необходимым личные встречи, он также затрудняет и усложняет их. Большинство активистов, с которыми разговаривала Amnesty International, были озабочены тем, что их мобильные телефоны могли использоваться для удалённой записи их встреч, или могли позволить определить их местоположение – и таким образом установить, с кем они встречаются. Кроме того, многие опасались, что в их офисах установлены прослушивающие устройства, из-за чего необходимо находить общественные места и там встречаться для обсуждений с глазу на глаз[…].

4.4 ВАЖНОСТЬ ШИФРОВАНИЯ

Тайное наблюдение и связанные с ним опасения делают использование шифрования крайне важным для белорусских журналистов, активистов и других жителей страны. Почти каждый, кто разговаривал с Amnesty International, особо выделял важность для своей работы шифрованных коммуникаций или устройств шифрования[…].

4.5 ОПРЕДЕЛЕНИЕ МЕСТОНАХОЖДЕНИЯ ТЕЛЕФОНА/ПРОСЛУШКА

Большая часть тех, с кем провела интервью Amnesty International, лично сталкивались с ситуациями (или что-то слышали о них), заставившими их подозревать, что телефоны прослушивались или отслеживались, хотя эти подозрения обычно невозможно было проверить[…].

4.6 ПРОСЛУШИВАНИЕ С ПОМОЩЬЮ «ЖУЧКОВ»/ФИЗИЧЕСКАЯ СЛЕЖКА

Физическая слежка, как и установка прослушивающих устройств, «жучков», в офисах и домах, по-прежнему вызывают опасения у многих представителей гражданского общества в Беларуси, затрудняя работу активистов и вынуждая их быть сдержанными при обсуждении важных вопросов в своих собственных офисах[…].

4.7 ВЗЛОМ

[…]Там, где случаи взлома, по всей видимости, действительно имели место, обычно не представляется возможным определить, с помощью каких средств был осуществлён взлом, или кем это было сделано. Зачастую эти случаи допускают различные технические объяснения. Как бы там ни было, следующие примеры показывают, что это может, тем не менее, затрагивать права активистов гражданского общества, когда частные имейлы или аккаунты в социальных сетях оказываются под угрозой.

ЛЕОНИД СУДАЛЕНКО

Многие из тех, кто разговаривал с Amnesty International, упоминали об одном эпизоде, который произошёл с Леонидом Судаленко. В январе 2015 года Судаленко, правозащитник из Гомеля, на юго-востоке Беларуси, обнаружил, что его учётная запись на mail.ru заблокирована: «Он [почтовый аккаунт на mail.ru] на самом деле был взломан дважды. В первый раз это произошло 6-го января, но тогда мне удалось восстановить его через службы технической поддержки и использовать дальше. Этот аккаунт был важен для меня: я создал его в 1999 году, когда ещё не было Gmail, это был мой официальный имейл, и за эти годы его узнали многие люди. Поэтому я не хотел удалять его, он был для меня ценным. Когда его взломали в первый раз, я восстановил его и пользовался им ещё две недели. Но когда 20-го числа его снова взломали, я потерял интерес к его использованию. Также я тогда решил, что нужно прекратить пользоваться аккаунтами, расположенными в России. Эти аккаунты не обеспечивают конфиденциальность. Их даже не надо взламывать: русская секретная служба могла легко передать мои пароли белорусской секретной службе». Ему удалось получить от Mail.ru документы, подтверждающие его усилия по восстановлению своей учётной записи электронной почты. Спустя несколько месяцев, в апреле, в его офис, который он использовал совместно со многими другими организациями гражданского общества, пришла милиция, которая изъяла восемь компьютеров (четыре забрали из офиса, и ещё четыре из дома, часть из них принадлежали его жене и детям) в связи с уголовным расследованием: «В тот день я был в Стокгольме. Шведские правозащитники пригласили меня на ежегодную международную правозащитную конференцию. В то время как я был там, мне позвонила жена и сказала, что у нас дома провели обыск, и что они искали не только порнографические материалы, но также и наркотики.

3 стр. >>>

Она сказал это, так как проводившие обыск милиционеры были из управления по наркоконтролю. Конечно, я был напуган. У меня двое сыновей-подростков, 14 и 18 лет. Была вероятность, что их как подростков подозревали в чём-то, связанном с наркотиками. Шведские правозащитники предложили мне ещё на некоторое время остаться в Стокгольме, однако я отказался и поехал в Беларусь, чтобы доказать свою невиновность. Вернувшись, я попытался выяснить, что произошло. Сегодня мне ясно, что это была спланированная провокацию с целью оклеветать меня. Я уверен, что если бы это не случилось прямо перед президентскими выборами 2015 года, я сейчас был бы в тюрьме. Статьи, по которым предполагалось обвинить меня, не предусматривают иных мер наказания, кроме тюремного заключения от 2 до 4 лет… Ситуация была следующая.

Порнография была отправлена с моего аккаунта (кстати, они послали её не только в налоговую службу, но и в районное следственное управление). Потом на основании этого факта было возбуждено уголовное дело. Требовалось расследовать этот вопрос. Так как порнография была послана с моего аккаунта, они пришли ко мне в офис и домой, чтобы провести там обыски. Они изъяли офисное оборудование. Я заявил, что это провокация с целью клеветы… После того, как они изъяли компьютеры, меня допросили в следственном управлении. Затем я показал следователю скриншоты, которые доказывали, что администрация mail.ru и я вели переписку по поводу этого взлома [аккаунта на mail.ru]. Позже, после июня 2015 года, была проведена экспертиза. Эксперт сказал, что порнографические материалы были посланы не с наших компьютеров. Потом они вернули нам компьютеры, и на этом всё кончилось. С тех пор следователи меня не беспокоили.

К тому времени многие национальные и международные организации выступили в мою защиту. Они написали президенту, начальнику КГБ и в Министерство внутренних дел. За меня вступились шведские правозащитники, Front Line Defenders и Amnesty International. Кроме того, более 25 известных белорусских правозащитников написали открытое письмо Министру внутренних дел, заявив, что знают меня как законопослушного гражданина и просят прекратить эту провокацию. Специальный докладчик по вопросу о положении правозащитников также был информирован об этой ситуации. Я думаю, что не получи я такой серьёзной поддержки, решение экспертов могло бы быть другим. Что значит экспертиза в Беларуси? Они всегда получают то, что им надо. Поэтому результаты экспертизы могли быть совершенно другими. И если бы эксперт заявил, что установил, что порнография была отправлена с моего компьютера, мне было бы тяжело доказать в суде свою невиновность».

4.8 КОНФИСКАЦИЯ

В то время как документально подтверждённые случаи взлома данных пользователей, возможно, сравнительно редки, конфискация компьютеров, телефонов и другого оборудования остаётся гораздо более распространённой угрозой для активистов, и в равной степени может обеспечить правительству доступ к персональным данным. Эксперты в области цифровой безопасности, с которыми разговаривала Amnesty International, считают конфискацию устройств наибольшей угрозой информационной безопасности, с которой сталкиваются активисты в Беларуси, и отмечают, что аресты, в результате которых никого не привлекали к суду, тем не менее могли сопровождаться конфискациями[…].

ЛЕОНИД СУДАЛЕНКО КОНФИСКАЦИЯ КОМПЬЮТЕРОВ

Правозащитник Леонид Судаленко заявил, что власти много раз конфисковывали компьютеры и другие устройства у него из дома и из офиса: «Обыски и конфискации, о которых идёт речь, происходили не впервые. Это был уже второй обыск, проведённый у меня дома, и пятый, устроенный в моём офисе. Они всегда изымали компьютеры, и всегда находили поводы для того, чтобы прийти и конфисковать наше офисное оборудование. Обычно они изымали наши компьютеры, изучали их примерно полгода, и затем возвращали. Некоторые компьютеры возвращали сломанными. Это всегда мешает рабочему процессу… [Возвращённые после конфискации компьютеры] мы не используем. И то же самое происходит, когда я пересекаю государственную границу. Например, последний раз это случилось в прошлом году, когда я возвращался в Минск из Вильнюса. Моё имя значилось в их базе данных. Посмотрев мой паспорт, они сразу же уводят меня в другую комнату, обыскивают и обычно забирают мой ноутбук, чтобы вернуть его примерно через шесть месяцев. Но я не буду пользоваться ноутбуком после этого, потому что к этому времени благодаря спонсорской программе у меня уже будет другой. Я имею в виду абсолютно новый, из магазина, запакованный в коробку, который можно использовать без опаски. Это происходило уже несколько раз, например, в прошлом году это случалось дважды – 24 мая и 25 августа. Оба раза меня тщательно обыскали, даже заставляли снимать носки. И оба раза они начинали обыскивать меня после того, как проверили мой паспорт».

4 стр. >>>

5. МЕЖДУНАРОДНОЕ ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ПРАВ ЧЕЛОВЕКА И СЛЕЖКА

Статья 17 Международного пакта о гражданских и политических правах (МПГПП) гласит, что «никто не может подвергаться произвольному или незаконному вмешательству в его личную или семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции», а также что «Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств»[…]. Слежка может нарушить права человека, даже если содержание коммуникаций не перехвачено, а также в случае, когда были перехвачены только сопутствующие данные – например, время, характер или местоположение коммуникации (так называемые «метаданные»). Как заметил Верховный комиссар ООН по правам человека, «накопление информации, которую обычно относят к «метаданным», может дать представление о поведении человека, его социальных отношениях, личных предпочтениях и индивидуальности, которое даже превосходит по значимости ту информацию, которую мог бы обеспечить доступ к личным коммуникациям».

В определённых обстоятельствах тайное наблюдение может быть совместимо с обязательствами в области прав человека, и может на самом деле служить важным и полезным инструментом в руках правоохранительных органов. Однако там, где национальная правовая база как таковая не может быть чётко определена или доступна общественности, или по каким-либо иным причинам не обеспечивает адекватные гарантии безопасности против злоупотреблений, а также там, где цели и характер слежки противоречит международным обязательствам государства в области прав человека, - в этих случаях слежка будет равноценна «произвольному и незаконному» посягательству на неприкосновенность частной жизни или иным образом будет нарушать права человека[…].



6. СЛЕЖКА ЗА КОММУНИКАЦИЯМИ В БЕЛАРУСИ: ЗАКОНЫ И ПРАКТИКА

4 декабря 2015 года Большая палата Европейского суда по правам человека (ЕСПЧ) вынесла решение по делу Роман Захаров против России, постановив, что российская система тайного наблюдения противоречит статье 8 Европейской конвенции о защите прав человека, защищающей право на частную и семейную жизнь. Хотя Беларусь не является участницей Европейской конвенции о защите прав человека, у белорусской и российской системы слежки, ставшей предметом дела Захарова, есть весьма много общего, поэтому решение по этому делу служит полезным ориентиром при анализе воздействия белорусской системы на права человека, особенно с учётом того, что права, о которых шла речь в деле Захарова, также защищаются договорами, участницей которых является Беларусь[…].

5 стр. >>>

6.1 ПРЯМОЙ ДОСТУП К ДАННЫМ КОММУНИКАЦИЙ

В деле Захарова ЕСПЧ критиковал действующую в России систему, которая даёт властям технические возможности получать прямой доступ к информации и данным без необходимости предъявлять разрешение суда компании-оператору услуг связи. Суд отметил: «по мнению Суда, такая система, как российская, которая позволяет спецслужбам и полиции непосредственно перехватывать коммуникации каждого гражданина без предъявления оператору услуг связи либо кому-то ещё санкции на такой перехват, особо располагает к произволу»[…].

В Беларуси нет общедоступной информации о том, как часто власти пользуются доступом к коммуникациям или связанным с ними данным. В ответ на просьбу Amnesty International предоставить эти статистические данные Департамент финансовых расследований Комитета государственного контроля заявил, что такие данные предоставить невозможно за их отсутствием, а также по той причине, что «некоторая информация, согласно законодательству Республики Беларусь, определяется как государственная тайна».

6.2 ХРАНЕНИЕ ДАННЫХ

В решении по делу Захарова ЕСПЧ отметил, что Суд Европейского союза (Суд ЕС) недавно критиковал директивы о всеохватном хранении данных — в решении от 8 апреля 2014 года по совместному делу Digital Rights Ireland and Seitinger and Others. Суд ЕС признал недействительной Директиву ЕС о хранении данных (2006/24/ЕС), которая требовала от операторов публичных услуг электронной связи либо публичных сетей связи хранить все данные о трафике и местоположении, но не содержание коммуникаций, от шести месяцев до двух лет. Суд ЕС признал, что хранение данных представляет собой серьёзное и масштабное нарушение основных прав, особенно права на частную жизнь, и отметил: «тот факт, что данные хранятся и впоследствии используются без уведомления абонента или зарегистрированного пользователя, с большой вероятностью вызовет у данных лиц ощущение того, что их частная жизнь постоянно находится под наблюдением»[…].

6.3 СФЕРА ПРИМЕНЕНИЯ МЕР ТАЙНОГО НАБЛЮДЕНИЯ

В решении по делу Захарова ЕСПЧ подчеркнул, что национальные законы должны соответствующим образом предусматривать обстоятельства, в которых могут применяться полномочия слежки. ЕСПЧ выразил тревогу, что слежку могут вести не только за подозреваемым в соответствии с российским законодательством, но также за «лицом, у которого может иметься информация об уголовном преступлении» либо за «лицом, у которого может быть информация, относящаяся к уголовному делу», причём ни то, ни другое не определяется законодательством[…].

В Беларуси слежка санкционируется в рамках Уголовно-процессуального кодекса (далее УПК) либо законом «Об оперативно-розыскной деятельности» (далее закон ОРД). Согласно статье 214 УПК, прослушивание и запись переговоров ограничиваются уголовными делами о тяжких и особо тяжких преступлениях. Однако такие действия применяются не только в отношении подозреваемых, но и «других лиц», если имеются достаточные основания полагать, что переговоры могут содержать сведения, имеющие значение для дела[…].

6.5 САНКЦИОНИРОВАНИЕ МЕР НАБЛЮДЕНИЯ

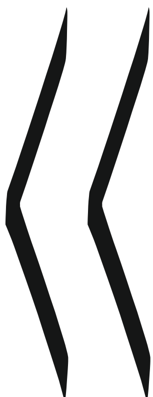
В решении по делу Захарова ЕСПЧ отметил, что российское требование судебной санкции на слежку является важной мерой защиты от произвола. Однако эту меру защиты подрывает ряд проблем, в том числе отсутствие требования к судьям проверять наличие разумных подозрений, а также необходимость и соразмерность этих мер. Кроме того, ЕСПЧ выразил тревогу в связи с отсутствием предусмотренного законом требования об указании конкретного лица или номера телефона в качестве объекта слежки.

Суд также критиковал тот факт, что в «неотложных» случаях для начала слежки не требуется санкция суда и что рассмотрение санкции в суде после последующего уведомления ограничивается лишь вопросом о продлении этой санкции, а не о том, была ли обоснована первоначальная санкция, либо о том, следует ли хранить или уничтожить собранные данные В Беларуси, согласно статье 19 закона ОРД, ряд видов оперативно-розыскных мероприятий, включая установку средств негласного наблюдения, прослушивающих устройств и контроль в сетях электросвязи или почтовых отправлений, требуют санкции прокурора или его заместителя, но не судьи[…].

При этом закон не требует от прокуроров, санкционирующих такие методы, проверять наличие разумных оснований либо необходимости и соразмерности, а также указывать конкретное лицо или адрес в качестве объекта слежки. В Беларуси также существуют целый ряд обстоятельств, при которых для ведения слежки не требуется даже санкции прокурора[…].

6 стр. >>>





6.6 НАДЗОР ЗА МЕРАМИ НАБЛЮДЕНИЯ

В решении по делу Захарова ЕСПЧ выразил тревогу отсутствием достаточного надзора за мерами наблюдения с целью предотвращения произвола[…]. ЕСПЧ отметил, что надзорным органам должны быть доступны все соответствующие документы, они должны обладать полномочиями, позволяющими устранять нарушения и должны быть открыты надзору, например, посредством публикации отчётов о своих надзорных функциях. Кроме того, суд счёл, что власти не представили примеров практических действий прокуроров по устранению нарушений.

В Беларуси прокурорам предоставлены определённые полномочия по надзору за оперативно-розыскными мероприятиями и расследованиями, однако закон не обязывает их пользоваться этими полномочиями[…].

6.7 ПРОДОЛЖИТЕЛЬНОСТЬ ТАЙНОГО НАБЛЮДЕНИЯ

В решении по делу Захарова ЕСПЧ подчеркнул, что для гарантии защиты от произвольной слежки в законе должен быть чётко прописан срок, по истечении которого ордер на перехват информации утрачивает силу, а также обстоятельства, позволяющие продлить действие такого ордера, и обстоятельства, требующие отмены ордера[…].

Статья 214 белорусского Уголовно-процессуального кодекса гласит: «О необходимости осуществления прослушивания и записи переговоров… орган дознания выносит мотивированное постановление, в котором указываются уголовное дело и основания… и в течение какого срока. Прослушивание и запись переговоров в любом случае не могут осуществляться свыше срока предварительного расследования уголовного дела и отменяются постановлением следователя, органа дознания».

Таким образом, хотя прослушивание по данной статье должно прекратиться по завершении предварительного следствия, статья не определяет ни возможную продолжительность прослушивания, ни необходимость продления соответствующего постановления[…].

6.8 ОБРАЩЕНИЕ С ДАННЫМИ

В решении по делу Захарова ЕСПЧ отметил, что закон должен предусматривать достаточные гарантии касательно хранения, доступа, рассмотрения, использования, обмена и уничтожения данных[…].

В Беларуси статьи 14 и 50 закона ОРД требуют от органов, осуществляющих оперативно-розыскную деятельность, не разглашать и не использовать во вред гражданам сведения, затрагивающие неприкосновенность частной жизни.

Органы, осуществляющие оперативно-розыскную деятельность, могут предоставлять в другой орган или международную организацию информацию, собранную в результате оперативно-розыскных мероприятий. Однако угроза сохранению в тайне личных сведений о гражданах может послужить основанием для отказа в предоставлении таких материалов.

Согласно статье 14 закона ОРД, власти должны уничтожать материалы оперативно-розыскной



деятельности, содержащие сведения, не связанные с противоправной деятельностью. Однако никакие конкретные сроки в этой связи не указаны и не упоминается, когда должны уничтожаться материалы оперативно-розыскных мероприятий, связанные с противоправной деятельностью, например, по завершении судебного разбирательства.

7 стр. >>>

6.9 УВЕДОМЛЕНИЕ О НАБЛЮДЕНИИ

В решении по делу Захарова ЕСПЧ отметил, что требование об уведомлении лиц о том, что за ними велось наблюдение, «неразрывно связано с эффективностью средств судебно-правовой защиты». Признав, что соблюдение секретности порой является ключевой составляющей слежки, суд, тем не менее, отметил: «Как только уведомление становится возможным без риска для цели ограничения по завершении мер наблюдения, информация об этом должна быть предоставлена всем заинтересованным лицам».

Законодательство Беларуси не требует уведомлять о слежке подвергающихся ей лиц[…].

8 ЗАКЛЮЧЕНИЕ

Белорусское законодательство позволяет властям прибегать к масштабной слежке практически по любой причине и не требует независимой судебной санкции или надзора[…]. Мобильные операторы и интернет-провайдеры, а также другие компании связи содействуют этому спорному прямому доступу властей к данным своих абонентов. Из-за полной секретности, окружающей практику слежки, о ней практически невозможно узнать, не говоря о том, чтобы опротестовать незаконную практику наблюдений[…].

Использование личных данных и коммуникаций с целью уголовного преследования людей после выборов 2010 года дало понять многим белорусам: они должны считать, что им постоянно грозит слежка.

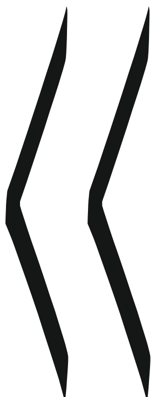
Это вредит гражданскому обществу Беларуси, которое и без того жёстко связано ограничительной правовой базой, регулирующей прочие аспекты их работы в стране. Поскольку такие законные действия, как действие от имени незарегистрированной организации или участие в мирном протесте могут повлечь уголовное преследование, многие активисты прибегают к самоцензуре и воздерживаются от реализации своих прав. Их законная работа в итоге становится всё труднее, поскольку такие простые задачи, как поиски финансирования для своей организации, телефонные звонки или организация встреч несут с собой риск — реальный или мнимый.

Хотя криптографическая защита и другие средства сохранения конфиденциальности могут помочь защитить некоторые личные данные, они не могут устранить риск слежки, с которым сталкиваются активисты. Мобильные телефоны всё также могут использоваться для прослушивания частных переговоров и определения местонахождения. Компьютеры и телефоны всё так же подвержены взломам, власти обладают полномочиями изымать устройства, а это приводит к тому, что активисты в дальнейшем боятся ими пользоваться.

Возникающий в итоге сковывающий эффект приводит к сужению пространства для гражданского общества и отрицательно воздействует на права человека в Беларуси, в том числе на право на информацию, поскольку всё меньше активистов, независимых журналистов и других могут представлять мнения, противоречащие официальным. Сковывающий эффект, возникающий в результате слежки — не случайность.

8 стр. >>>

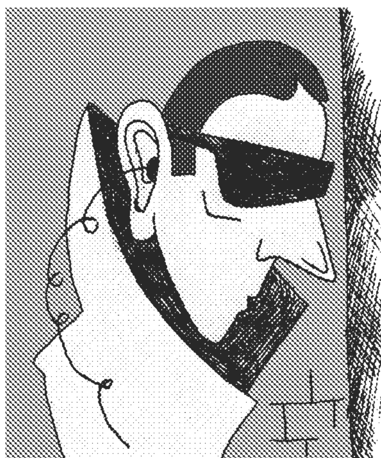




9 РЕКОМЕНДАЦИИ
9.1 ИСПОЛНИТЕЛЬНОЙ И ЗАКОНОДАТЕЛЬНОЙ ВЕТВЯМ ПРАВИТЕЛЬСТВА РЕСПУБЛИКИ БЕЛАРУСЬ

1. Реформировать законодательство, относящееся к слежке, в том числе закон «Об оперативно-розыскной деятельности» (№ 307-З от 15 июля 2015 года) и Уголовный кодекс, приведя правовой режим и относящуюся к нему практику в соответствие с нормами и стандартами международного права в области прав человека.

2. Обеспечить, чтобы общественности была доступна информация, относящаяся к законам и практике касательно слежки как минимум в той мере, которая предусмотрена Глобальными принципами национальной безопасности и правом на информацию (принципами Тсване).

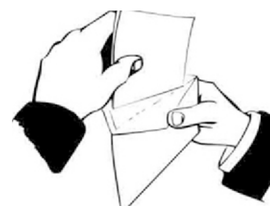


3. Помимо прочего следует принять меры, нацеленные на обеспечение следующего:

 государственные органы должны предъявлять утверждённые судом запросы о предоставлении им телекоммуникационных данных, а не пользоваться прямым, удалённо контролируемым доступом;
 от поставщиков телекоммуникационных услуг не следует требовать сохранять данные коммуникаций вне условий уголовного расследования, а лишь на основании судебного ордера, содержащего надлежащую информацию о конкретном лице и разумные подозрения в совершении противоправных действий;
 перехват сообщений и доступ к связанным с ними данным допускается только при наличии санкции, выданной или соответственно продлённой независимым судебным органом, который должен оценить наличие конкретных разумных подозрений в совершении противоправных действий лицом, подвергающимся слежке; судебный орган должен быть удовлетворён, что при этом соблюдены критерии необходимости и соразмерности;
 правовые основания тайного наблюдения, в том числе определение национальной безопасности, надлежит включить в законодательство и определить их столь подробно и узко, чтобы они отвечали стандарту ясности и точности и были бы достаточны для разъяснения лицам обстоятельств, которые могут привести к слежке;
 полномочия по проведению тайного наблюдения должны подлежать надзору со стороны действительно независимого надзорного органа, обладающего достаточной материальной базой, прозрачного для общественности, имеющего доступ ко всей информации и обладающего полномочиями и мандатом выявлять, расследовать и прекращать тайную слежку, а также предоставлять средства правовой защиты в случаях связанных с ней нарушений прав человека;
 внести поправки в законодательство, чётко ограничив продолжительность тайного наблюдения во всех случаях;
 законодательно предусмотреть требования об уничтожении всех связанных со слежкой данных;
 лиц, подвергающихся слежке, следует уведомлять о том, что за ними следили, если это не противоречит или более не противоречит законной цели текущего расследования;
 обеспечить доступ к средствам эффективной правовой защиты и позволить гражданам опротестовывать меры наблюдения либо нарушения своих прав в связи со слежкой в независимом суде со всеми необходимыми гарантиями надлежащего процесса;
 предать огласке достаточную информацию о технических данных систем слежки, включая средства взлома.

https://www.amnesty.org/en/documents/eur49/4306/2016/ru/

Информационно-аналитический бюллетень Гомельского Центра стратегической тяжбы
"Стратегическая тяжба"



Редактор Алексей Коваль
а/я 28, 246003, Гомель. Тираж 299 экз.
Отпечатано на личном оборудовании.
Распространяется бесплатно.